

(19)



JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **09298736 A**

(43) Date of publication of application: **18 . 11 . 97**

(51) Int. Cl.

H04N 7/167
G09C 1/00
H04L 9/22
H04L 9/36

(21) Application number: **08113598**

(22) Date of filing: **08 . 05 . 96**

(71) Applicant: **MATSUSHITA ELECTRIC IND CO LTD**

(72) Inventor: **HATAKEYAMA TAKESHI**
MURAKAMI HIRONORI
KATSUTA NOBORU
IBARAKI SUSUMU

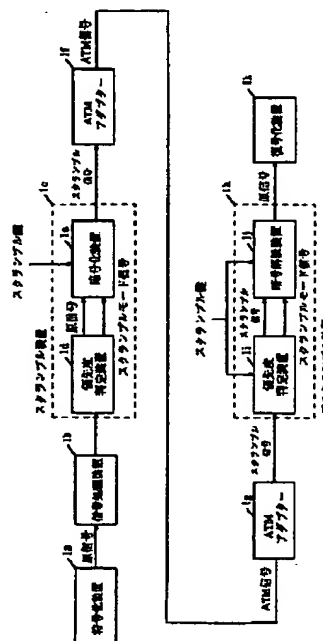
(54) **SCRAMBLE TRANSMITTER, SCRAMBLER, DESCRAMBLER AND SIGNAL PROCESSOR**

(57) Abstract:

PROBLEM TO BE SOLVED: To realize effect control and reduction on packet abort in the scramble transmitter to limit a party to reproduce digital coded data with priority.

SOLUTION: A scrambler 1c conducts scrambling by revising the scramble mode depending on priority relating to packet abort to obtain a scramble signal. A descrambler 1h conducts processing reverse to above to obtain a reproduction signal. Through the constitution above, scrambling is applied to packets with low priority to realize effect control or series of ciphers with a chain are divided depending on the priority to reduce the effect on packet abort.

COPYRIGHT: (C)1997,JPO



(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平9-298736

(43)公開日 平成9年(1997)11月18日

(51)Int.Cl. ⁶	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 N 7/167			H 0 4 N 7/167	Z
G 0 9 C 1/00	6 6 0	7259-5 J	G 0 9 C 1/00	6 6 0 E
H 0 4 L 9/22			H 0 4 L 9/00	6 5 5
9/36				6 8 5

審査請求 未請求 請求項の数23 O L (全 19 頁)

(21)出願番号 特願平8-113598

(22)出願日 平成8年(1996)5月8日

(71)出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72)発明者 畠山 武士

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72)発明者 村上 弘規

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72)発明者 勝田 昇

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(74)代理人 弁理士 岡田 和秀

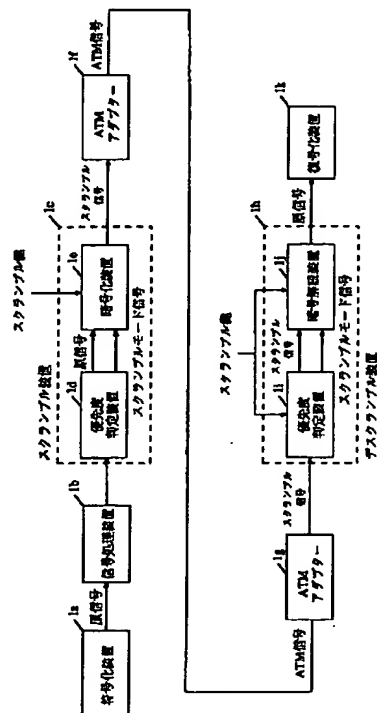
最終頁に続く

(54)【発明の名称】 スクランブル伝送装置およびスクランブル装置およびデスクランブル装置および信号処理装置

(57)【要約】

【課題】 優先度を有するデジタル符号化されたデータの再生に際して、その再生者を限定するためのスクランブル伝送装置に関するもので、効果制御やパケット廃棄への影響の低減を実現するスクランブル伝送装置を提供する。

【解決手段】 スクランブル装置1cは、パケット廃棄に関する優先度に応じてスクランブルモードを変更してスクランブルを行い、スクランブル信号を得る。デスクランブル装置1hでは、逆処理を行い、再生信号を得る。このような構成により、低優先度のパケットにのみスクランブルを行い、効果制御を実現したり、優先度に応じて連鎖のある暗号の系列を分け、パケット廃棄への影響を低減したスクランブル伝送装置を実現する。



【特許請求の範囲】

【請求項1】 スクランブル装置とデスクランブル装置とを具備し、前記スクランブル装置は、パケット廃棄に関する優先度に応じて異なるスクランブルモードでスクランブルを行うように構成され、前記デスクランブル装置は、前記スクランブル装置からのデータについて前記パケット廃棄に関する優先度に応じて前記異なるスクランブルモードでデスクランブルを行うように構成されていることを特徴とするスクランブル伝送装置。

【請求項2】 スクランブル装置が優先度判定装置と暗号化装置とを具備し、前記優先度判定装置は、パケット廃棄に関する優先度を有するパケットを入力とし、前記パケット廃棄に関する優先度を判定し、前記暗号化装置にパケットとスクランブルモード信号を出力するように構成され、前記暗号化装置は、前記優先度判定装置からの前記スクランブルモード信号に基づきスクランブルを行うように構成されていることを特徴とする請求項1に記載のスクランブル伝送装置。

【請求項3】 デスクランブル装置が優先度判定装置と暗号解読装置とを具備し、前記優先度判定装置は、パケット廃棄に関する優先度を有するパケットを入力とし、前記パケット廃棄に関する優先度を有するパケットの優先度を判定し、前記暗号解読装置にパケットとスクランブルモード信号を出力するように構成され、前記暗号解読装置は、前記優先度判定装置からの前記スクランブルモード信号に基づきデスクランブルを行うように構成されていることを特徴とする請求項1に記載のスクランブル伝送装置。

【請求項4】 スクランブル装置は、パケット廃棄に関する優先度が高優先度のパケットについてはスクランブルを行わず、前記パケット廃棄に関する優先度が低優先度のパケットについてはスクランブルを行うように構成されていることを特徴とする請求項1に記載のスクランブル伝送装置。

【請求項5】 デスクランブル装置は、スクランブル鍵を有する場合には、パケット廃棄に関する優先度が高優先度のパケットについては処理を行わず、前記パケット廃棄に関する優先度が低優先度のパケットについてはデスクランブルを行い、かつ、前記スクランブル鍵を有しない場合には、前記パケット廃棄に関する優先度が高優先度のパケットについては処理を行わず、前記パケット廃棄に関する優先度が低優先度のパケットについては廃棄を行うように構成されていることを特徴とする請求項1に記載のスクランブル伝送装置。

【請求項6】 スクランブル装置は、連鎖のある暗号方式でスクランブルを行い、パケット廃棄に関する優先度が高優先度のパケットと低優先度のパケットとを別々の前記連鎖のある暗号方式の系列としてスクランブルを行うように構成されていることを特徴とする請求項1に記載のスクランブル伝送装置。

【請求項7】 デスクランブル装置は、連鎖のある暗号方式でデスクランブルを行い、パケット廃棄に関する優先度が高優先度のパケットと低優先度のパケットとを別々の前記連鎖のある暗号方式の系列としてデスクランブルを行うように構成されていることを特徴とする請求項1に記載のスクランブル伝送装置。

【請求項8】 2つの連続するパケットを単位として処理を行い、2つのパケットのうち一方のパケットのパケット廃棄に関する優先度が高優先度のパケットの場合には2つのパケットの両方を高優先度のパケットに書き換えて出力する信号処理装置を付加していることを特徴とする請求項1に記載のスクランブル伝送装置。

【請求項9】 パケット廃棄に関する優先度が、MP EG 2トランスポートストリームにおけるトランスポートパケットの優先度を示す1ビットのフラグtransport _priorityであることを特徴とする請求項1に記載のスクランブル伝送装置。

【請求項10】 パケット廃棄に関する優先度に応じて異なるスクランブルモードでスクランブルを行うように構成されていることを特徴とするスクランブル装置。

【請求項11】 優先度判定装置と暗号化装置とを具備し、前記優先度判定装置は、パケット廃棄に関する優先度を有するパケットを入力とし、入力されたパケットの前記パケット廃棄に関する優先度を判定し、前記暗号化装置にパケットとスクランブルモード信号を出力するように構成され、前記暗号化装置は、前記優先度判定装置からの前記スクランブルモード信号に基づきスクランブルを行うように構成されていることを特徴とする請求項10に記載のスクランブル装置。

【請求項12】 パケット廃棄に関する優先度が高優先度のパケットについてはスクランブルを行わず、前記パケット廃棄に関する優先度が低優先度のパケットについてはスクランブルを行うように構成されていることを特徴とする請求項10に記載のスクランブル装置。

【請求項13】 連鎖のある暗号方式でスクランブルを行い、パケット廃棄に関する優先度が高優先度のパケットと低優先度のパケットとを別々の前記連鎖のある暗号方式の系列としてスクランブルを行うように構成されていることを特徴とする請求項10に記載のスクランブル装置。

【請求項14】 パケット廃棄に関する優先度が、MP EG 2トランスポートストリームにおけるトランスポートパケットの優先度を示す1ビットのフラグtransport _priorityであることを特徴とする請求項10に記載のスクランブル装置。

【請求項15】 パケット廃棄に関する優先度に応じて異なるスクランブルモードでデスクランブルを行うように構成されていることを特徴とするデスクランブル装置。

【請求項16】 優先度判定装置と暗号解読装置とを具

備し、前記優先度判定装置は、パケット廃棄に関する優先度を有するパケットを入力とし、入力されたパケットの前記パケット廃棄に関する優先度を判定し、前記暗号解読装置にパケットとスクランブルモード信号を出力するように構成され、前記暗号解読装置は、前記優先度判定装置からの前記スクランブルモード信号に基づきデスクランブルを行うように構成されていることを特徴とする請求項15に記載のデスクランブル装置。

【請求項17】 スクランブル鍵を有する場合には、パケット廃棄に関する優先度が高優先度のパケットについては処理を行わず、前記パケット廃棄に関する優先度が低優先度のパケットについてはデスクランブルを行い、かつ、前記スクランブル鍵を有しない場合には、前記パケット廃棄に関する優先度が高優先度のパケットについては処理を行わず、前記パケットに関する優先度が低優先度のパケットについては廃棄を行うように構成されていることを特徴とする請求項15に記載のデスクランブル装置。

【請求項18】 連鎖のある暗号方式でデスクランブルを行い、パケット廃棄に関する優先度が高優先度のパケットと低優先度のパケットとを別々の前記連鎖のある暗号方式の系列としてデスクランブルを行うように構成されていることを特徴とする請求項15に記載のデスクランブル装置。

【請求項19】 パケット廃棄に関する優先度が、MP EG2トランスポートストリームにおけるトランスポートパケットの優先度を示す1ビットのフラグtransport _priorityであることを特徴とする請求項15に記載のデスクランブル装置。

【請求項20】 パケット廃棄に関する優先度を有するパケットを入力とし、入力された2つの連続するパケットを単位として処理を行い、2つのパケットのうち一方のパケットのパケット廃棄に関する優先度が高優先度のパケットの場合には2つのパケットの両方を高優先度のパケットに書き換えてスクランブル装置に出力するように構成されていることを特徴とするスクランブル伝送装置用の信号処理装置。

【請求項21】 パケット廃棄に関する優先度が、MP EG2トランスポートストリームにおけるトランスポートパケットの優先度を示す1ビットのフラグtransport _priorityであることを特徴とする請求項20に記載のスクランブル伝送装置用の信号処理装置。

【請求項22】 2つの連続するパケットを単位として処理を行うことに代えて、3つ以上の連続するパケットを単位として処理を行うように構成してあることを特徴とする請求項8に記載のスクランブル装置。

【請求項23】 2つの連続するパケットを単位として処理を行うことに代えて、3つ以上の連続するパケットを単位として処理を行うように構成してあることを特徴とする請求項20のスクランブル伝送装置用の信号処理

装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、ディジタル符号化されたデータの伝送に際し、信号をスクランブルし、デスクランブル手順を許可されたものだけに与えることによって、再生できる者を限定するスクランブル伝送装置、およびこのスクランブル伝送装置を構成するスクランブル装置、およびデスクランブル装置、およびパケット廃棄に関する優先度の変換を行う信号処理装置に関するものであって、パケット廃棄に関する優先度を用いることによって、効果制御、パケット廃棄によるエラー伝搬の低減などを実現するスクランブル伝送装置、スクランブル装置、デスクランブル装置、信号処理装置に関するものである。

【0002】

【従来の技術】 従来のディジタル信号に対するスクランブル伝送装置としては、連鎖のあるブロック暗号方式により入力信号を暗号化する方法があった。たとえば、「現代暗号理論」（電子情報通信学会編）第4章に、連鎖のあるブロック暗号方式を用いた暗号化方法に関する記述がある。

【0003】 ブロック暗号方式とは、暗号化するデータを固定長のブロックに分解して、ブロックごとに暗号化する方式であり、連鎖のあるブロック暗号方式とは、ブロックの暗号化がそのブロックの前のブロックに依存する方式である。

【0004】 連鎖のあるブロック暗号方式の1例として、暗号文ブロック連鎖方式（CBCモード）について説明する。

【0005】 図9は、このような暗号文ブロック連鎖方式（CBCモード）を用いた従来のディジタルスクランブル伝送装置の構成図である。ここで、2aはスクランブル装置、2eはデスクランブル装置、2b、2fはCBCレジスタ、2c、2gは排他的論理和回路、2dはブロック暗号化器、2hはブロック復号化器である。

【0006】 以上のように構成された従来例について、以下にその動作を説明する。スクランブル装置2aにおいて原信号 M_i が入力される。スクランブル装置2aは、この原信号 M_i を決まったビット数のブロックに分割し、ブロック単位でスクランブルを行う。スクランブルはスクランブル鍵をもとにブロック暗号化器2dで行われる。このようなブロックごとに分割し暗号化する方式がブロック暗号方式であるが、このとき、安全性を高めるために、以下に説明する暗号文ブロック連鎖方式（CBCモード）が用いられる。

【0007】 CBCレジスタ2bを用意しておき、このレジスタに1つ前のスクランブル装置2aの出力 C_{i-1} を記憶するようにする。また、CBC初期値には、スクランブル装置2aとデスクランブル装置2eに共通の値 V を準備

し、初期時にロードする。排他的論理和回路2cにおいて、CBCレジスタ2bの出力 C_{i-1} と原信号 M_i の排他的論理和の演算を行い、ブロック暗号化器2dに出力する。ブロック暗号化器2dは、排他的論理和回路2cからの信号を、スクランブル鍵をもとに暗号化を行い、スクランブル装置2aの出力としてスクランブル信号 C_i を出力する。ブロック暗号化器2dで行われる暗号化の関数を E_i とすると、スクランブル信号 C_i は、 $C_i = E_i (M_i \text{「+」 } C_{i-1})$ と表すことができる。ここで、記号「+」は排他的論理和を示す。

【0008】一方、デスクランブル装置2eでは、スクランブル装置2aと逆の処理を行う。すなわち、ブロック復号化器2hにおいて、スクランブル信号 C_i が決まったビット長のブロックに分割され、復号が行われる。このときブロック復号装置2hで行われる処理 D_i は、ブロック暗号化器2dで行われる処理 E_i の逆の処理であり、 $D_i (E_i (M_i)) = M_i$ となるものである。

【0009】以下、デスクランブル装置2eにおける暗号文ブロック連鎖方式(CBCモード)について説明する。

【0010】CBCレジスタ2fにおいて、1つ前のスクランブル信号 C_{i-1} を記憶し、排他的論理和回路2gに出力を行う。また、初期時には、スクランブル装置2aと共通の初期値VをCBCレジスタ2fにロードする。ブロック復号化器2hは、スクランブル信号 C_i を入力とし、スクランブル鍵をもとに復号を行い、排他的論理和回路2gに出力を行う。排他的論理和回路2gは、CBCレジスタ2fの出力 C_{i-1} とブロック復号化器2hの出力 $D_i (C_i)$ の排他的論理和の演算を行い、デスクランブル装置2eの出力として出力する。このときブロック復号化器2hの処理を D_i とすると、復号信号は、 $D_i (C_i) \text{「+」 } C_{i-1} = M_i \text{「+」 } C_{i-1} \text{「+」 } C_{i-1} = M_i$

と表すことができ、原信号 M_i となることが分かる。ここで、記号「+」は排他的論理和を示す。

【0011】

【発明が解決しようとする課題】しかしながら前記のような構成では、以下のような2つの課題があった。

【0012】第1の課題は、映像信号や音声信号において、ブロック暗号を用いる場合に、攪拌の程度を制御する効果制御が困難であるという課題である。

【0013】効果制御というのは、正規の受信者が高解像度の画像を視聴できることに加えて正規の受信者以外の受信者でも低解像度の画像を視聴できるようにすることである。入力信号が映像や音声の単に各画像の画素のサンプル値や各音声の音素のサンプル値を示す信号であれば、OFBモードと呼ばれるブロック暗号の方式を用いることにより疑似乱数を発生させ、疑似乱数の1と0

のビット数の割合を制御することにより、正規の受信者以外が受信できる映像、音声信号の攪拌の程度を制御できる効果制御(低解像度の画像を表示すること)を行うことができるが、通常、デジタル信号を伝送、記録する際には、高能率符号化を行うことが多く、このような高能率符号化された信号の場合には、数ビットの信号を反転するだけで他の部分も解読困難となり、攪拌の程度を制御する効果制御が困難である(画像がどのようなものであるか全く分からなくなる)という問題がある。

【0014】本発明はかかる点に鑑み、高能率符号化された信号に対する効果制御を容易に実現可能なスクランブル伝送装置、およびそのスクランブル装置、デスクランブル装置を提供することを目的とする。

【0015】第2の課題は、ATMネットワークなどのパケット廃棄が発生するネットワークにおけるセル廃棄による影響の伝搬の問題である。

【0016】この課題の1つ目の例を図10を用いて説明する。図10はパケット廃棄による影響の伝搬の説明図である。図10において、3a、3cは優先パケット、3b、3dは非優先パケットである。

【0017】ATM伝送(Asynchronous Transfer Mode: 非同期転送モード)などの伝送方式によって伝送を行った場合には、ネットワークにおいて非優先パケットの廃棄が行われるが、連鎖のある暗号を用いた場合、すなわち、スクランブルおよびデスクランブルが、対象となるブロックの前のブロックに依存した暗号方式を用いる場合に、非優先パケットの廃棄が行われたとき、そのパケットの次のパケットはデスクランブルが不可能となる。このように、パケット廃棄により非優先パケットの廃棄が行われた場合、次のパケットが復号できないため、そのパケットが重要なパケットである優先パケットであった場合には影響が大きいという問題がある。

【0018】次に、図6を用いて、第2の課題の2つ目の例について説明する。図6はMPEG over ATMのAAL5による方式の説明図である。図6において、4a、4bはMPEG 2標準に準拠したトランスポートパケット、4cはATM AAL5におけるCPCS-PDUトレーラー、4d、4e、4f、4g、4h、4i、4j、4kはATMセルである。図6はMPEG 2のトランスポートパケットをATMセルで伝搬する際の方法を示すものであり、トランスポートパケット4a、4bの2つにCRCを含むCPCS-PDUトレーラー4cを加えたものを8つのATMセル4d、4e、4f、4g、4h、4i、4j、4kのペイロードに割り当てる。

【0019】この例の場合、1つのATMセルが廃棄により失われると、そのATMセルを含むトランスポートパケット2つについてCRCのチェックがエラーとなるため復号不可能となり、更にその次のトランスポートパケット1つがデスクランブル不可能となるため、3つのトランスポートパケットが失われることになる。このよ

うに、複数パケットを単位として処理している場合には、1つのパケット廃棄により失われるパケットの数が大きく、パケット廃棄の問題は大きい。

【0020】本発明はかかる点に鑑み、パケット廃棄の影響の低減を実現可能なスクランブル伝送装置、およびそのスクランブル装置、デスクランブル装置、信号処理装置を提供することを目的とする。

【0021】

【課題を解決するための手段】本発明に係るスクランブル伝送装置は、パケット廃棄に関する優先度をもつパケットにより構成される信号を入力とし、優先度に応じてスクランブルモードの切り換えを行ってスクランブルを行うスクランブル装置と、スクランブル装置からのスクランブル信号を入力とし、優先度に応じてスクランブルモードの切り換えを行ってデスクランブルを行うデスクランブル装置とから構成されていることを特徴としている。パケット廃棄に関する優先度によりスクランブルモードを変更することによって、効果制御を実現できるとともに、パケット廃棄に対する影響を低減することができる。

【0022】また、本発明に係るスクランブル伝送装置は、パケット廃棄に関する優先度をもつパケットにより構成される信号を入力とし、優先度の高いパケットについてはスクランブルを行わず、優先度の低いパケットについてはスクランブルを行うスクランブル装置と、スクランブル装置からのスクランブル信号を入力とし、スクランブル鍵が存在する場合には優先度の低いパケットについてのみデスクランブルを行い、スクランブル鍵が存在しない場合には優先度の低いパケットを廃棄するデスクランブル装置とから構成されていることを特徴としている。スクランブル装置においてパケット廃棄に関する優先度が低いパケットのみをスクランブルし、デスクランブル装置において、スクランブル鍵が存在する場合、すなわち視聴などの契約を行っている場合にはデスクランブルを行い、スクランブル鍵が存在しない場合、すなわち視聴などの契約を行っていない場合にはデスクランブル不可能な優先度の低いパケットは廃棄する。このようにすることによって、正規の受信者は優先度の高いパケットと優先度の低いパケットの両方を復号することができ、正規の受信者以外の受信者は優先度の高いパケットのみを復号することができる。従って、例えば原信号がデジタル映像信号のような信号の場合に、優先度の高いパケットに画像の低解像度の情報を、優先度の低いパケットに画像の低解像度の情報に追加する高解像度の情報をそれぞれ割り当てることによって、正規の受信者以外の受信者も低解像度の画像を視聴することが可能な効果制御を実現することができる。

【0023】また、本発明に係るスクランブル伝送装置は、パケット廃棄に関する優先度をもつパケットにより構成される信号を入力とし、優先度の高いパケットと優

先度の低いパケットを別々の連鎖のある暗号方式の系列としてスクランブルを行うスクランブル装置と、スクランブル装置からのスクランブル信号を入力とし、優先度の高いパケットと優先度の低いパケットを別々の連鎖のある暗号方式の系列としてデスクランブルを行うデスクランブル装置とから構成されていることを特徴としている。パケット廃棄に関する優先度の高いパケットと低いパケットを別々の連鎖のある暗号方式の系列としてスクランブルすることによって、ネットワーク中で優先度の低いパケットの廃棄が行われた場合にでも、優先度の高いパケットに影響を及ぼさないようにすることが可能となり、パケット廃棄への影響を低減することができる。

【0024】また、本発明に係るスクランブル伝送装置は、パケット廃棄に関する優先度をもつパケットにより構成される信号を入力とし、2つの連続するパケットを単位として処理し、2つのパケットのうち一方が優先度の高いパケットの場合には、両方とも優先度の高いパケットに書き換えて出力する信号処理装置と、信号処理装置からの信号を入力とし、優先度の高いパケットと優先度の低いパケットを別々の連鎖のある暗号方式の系列としてスクランブルを行うスクランブル装置と、スクランブル装置からのスクランブル信号を入力とし、優先度の高いパケットと優先度の低いパケットを別々の連鎖のある暗号方式の系列としてデスクランブルを行うデスクランブル装置とから構成されていることを特徴としている。2つずつの連続したパケットを単位として処理を行うスクランブル伝送装置において、2つのパケットのうち一方が優先度の高いパケットの場合に両方とも優先度の高いパケットに書き換え、優先度の高いパケット単位と優先度の低いパケット単位とを別々の連鎖のある暗号方式の系列としてスクランブルし、優先度の低いパケットの廃棄の影響を低減することができる。すなわち、優先度の低いパケットの廃棄が行われた場合も、同じパケット単位内には優先度の高いパケットは含まれないため、同じパケット単位内の優先度の高いパケットには影響がなく、優先度の高いパケット単位とは別の連鎖のある暗号方式の系列のため、次のパケット単位の優先度の高いパケットにも影響がない。

【0025】

【発明の実施の形態】本発明に係る請求項1のスクランブル伝送装置は、スクランブル装置とデスクランブル装置とを具備し、前記スクランブル装置は、パケット廃棄に関する優先度に応じて異なるスクランブルモードでスクランブルを行うように構成され、前記デスクランブル装置は、前記スクランブル装置からのデータについて前記パケット廃棄に関する優先度に応じて前記異なるスクランブルモードでデスクランブルを行うように構成されていることを特徴としている。パケット廃棄に関する優先度によりスクランブルモードを変更することによって、効果制御を実現できるとともに、パケット廃棄に対

10

20

30

40

50

する影響を低減することができる。

【0026】本発明に係る請求項2のスクランブル伝送装置は、上記請求項1において、スクランブル装置が優先度判定装置と暗号化装置とを具備し、前記優先度判定装置は、パケット廃棄に関する優先度を有するパケットを入力とし、前記パケット廃棄に関する優先度を判定し、前記暗号化装置にパケットとスクランブルモード信号を出力するように構成され、前記暗号化装置は、前記優先度判定装置からの前記スクランブルモード信号に基づきスクランブルを行うように構成されていることを特徴としている。効果制御を実現できるとともに、パケット廃棄に対する影響を低減できる。

【0027】本発明に係る請求項3のスクランブル伝送装置は、上記請求項1において、デスクランブル装置が優先度判定装置と暗号解読装置とを具備し、前記優先度判定装置は、パケット廃棄に関する優先度を有するパケットを入力とし、前記パケット廃棄に関する優先度を有するパケットの優先度を判定し、前記暗号解読装置にパケットとスクランブルモード信号を出力するように構成され、前記暗号解読装置は、前記優先度判定装置からの前記スクランブルモード信号に基づきデスクランブルを行うように構成されていることを特徴としている。効果制御を実現できるとともに、パケット廃棄に対する影響を低減できる。

【0028】本発明に係る請求項4のスクランブル伝送装置は、上記請求項1において、スクランブル装置は、パケット廃棄に関する優先度が高優先度のパケットについてはスクランブルを行わず、前記パケット廃棄に関する優先度が低優先度のパケットについてはスクランブルを行うように構成されていることを特徴としている。

【0029】優先度の高いパケットに画像の低解像度の情報を、優先度の低いパケットに画像の低解像度の情報に追加する高解像度の情報をそれぞれ割り当てることによって、正規の受信者以外の受信者も低解像度の画像を視聴することが可能な効果制御を実現できる。

【0030】本発明に係る請求項5のスクランブル伝送装置は、上記請求項1において、デスクランブル装置は、スクランブル鍵を有する場合には、パケット廃棄に関する優先度が高優先度のパケットについては処理を行わず、前記パケット廃棄に関する優先度が低優先度のパケットについてはデスクランブルを行い、かつ、前記スクランブル鍵を有しない場合には、前記パケット廃棄に関する優先度が高優先度のパケットについては処理を行わず、前記パケット廃棄に関する優先度が低優先度のパケットについては廃棄を行うように構成されていることを特徴としている。優先度の高いパケットに画像の低解像度の情報を、優先度の低いパケットに画像の低解像度の情報に追加する高解像度の情報をそれぞれ割り当てることによって、正規の受信者以外の受信者も低解像度の画像を視聴することが可能な効果制御を実現できる。

【0031】本発明に係る請求項6のスクランブル伝送装置は、上記請求項1において、スクランブル装置は、連鎖のある暗号方式でスクランブルを行い、パケット廃棄に関する優先度が高優先度のパケットと低優先度のパケットとを別々の前記連鎖のある暗号方式の系列としてスクランブルを行うように構成されていることを特徴としている。パケット廃棄に関する優先度の高いパケットと低いパケットを別々の連鎖のある暗号方式の系列としてスクランブルすることによって、ネットワーク中で優先度の低いパケットの廃棄が行われた場合にも、優先度の高いパケットに影響を及ぼさないようにすることが可能となり、パケット廃棄への影響を低減することができる。

【0032】本発明に係る請求項7のスクランブル伝送装置は、上記請求項1において、デスクランブル装置は、連鎖のある暗号方式でデスクランブルを行い、パケット廃棄に関する優先度が高優先度のパケットと低優先度のパケットとを別々の前記連鎖のある暗号方式の系列としてデスクランブルを行うように構成されていることを特徴としている。パケット廃棄に関する優先度の高いパケットと低いパケットを別々の連鎖のある暗号方式の系列としてデスクランブルすることによって、ネットワーク中で優先度の低いパケットの廃棄が行われた場合にも、優先度の高いパケットに影響を及ぼさないようにすることが可能となり、パケット廃棄への影響を低減することができる。

【0033】本発明に係る請求項8のスクランブル伝送装置は、上記請求項1において、2つの連続するパケットを単位として処理を行い、2つのパケットのうち一方のパケットのパケット廃棄に関する優先度が高優先度のパケットの場合には2つのパケットの両方を高優先度のパケットに書き換えて出力する信号処理装置を付加していることを特徴としている。優先度の高いパケット単位と優先度の低いパケット単位とを別々の連鎖のある暗号方式の系列としてスクランブルし、優先度の低いパケットの廃棄の影響を低減することができる。

【0034】本発明に係る請求項9のスクランブル伝送装置は、上記請求項1において、パケット廃棄に関する優先度が、MPEG2トランスポートストリームにおけるトランスポートパケットの優先度を示す1ビットのフラグtransport __priorityであることを特徴としている。効果制御を実現できるとともに、パケット廃棄に対する影響を低減できる。

【0035】本発明に係る請求項10のスクランブル装置は、パケット廃棄に関する優先度に応じて異なるスクランブルモードでスクランブルを行うように構成されていることを特徴としている。パケット廃棄に関する優先度によりスクランブルモードを変更することによって、効果制御を実現できるとともに、パケット廃棄に対する影響を低減することができる。

【0036】本発明に係る請求項11のスクランブル伝送装置は、上記請求項10において、優先度判定装置と暗号化装置とを具備し、前記優先度判定装置は、パケット廃棄に関する優先度を有するパケットを入力とし、入力されたパケットの前記パケット廃棄に関する優先度を判定し、前記暗号化装置にパケットとスクランブルモード信号を出力するように構成され、前記暗号化装置は、前記優先度判定装置からの前記スクランブルモード信号に基づきスクランブルを行うように構成されていることを特徴としている。効果制御を実現できるとともに、パケット廃棄に対する影響を低減できる。

【0037】本発明に係る請求項12のスクランブル装置は、上記請求項10において、パケット廃棄に関する優先度が高優先度のパケットについてはスクランブルを行わず、前記パケット廃棄に関する優先度が低優先度のパケットについてはスクランブルを行うように構成されていることを特徴としている。優先度の高いパケットに画像の低解像度の情報を、優先度の低いパケットに画像の低解像度の情報に追加する高解像度の情報をそれぞれ割り当てることによって、正規の受信者以外の受信者も低解像度の画像を視聴することが可能な効果制御を実現できる。

【0038】本発明に係る請求項13のスクランブル装置は、上記請求項10において、連鎖のある暗号方式でスクランブルを行い、パケット廃棄に関する優先度が高優先度のパケットと低優先度のパケットとを別々の前記連鎖のある暗号方式の系列としてスクランブルを行うように構成されていることを特徴としている。パケット廃棄に関する優先度の高いパケットと低いパケットを別々の連鎖のある暗号方式の系列としてスクランブルすることによって、ネットワーク中で優先度の低いパケットの廃棄が行われた場合にでも、優先度の高いパケットに影響を及ぼさないようにすることが可能となり、パケット廃棄への影響を低減することができる。

【0039】本発明に係る請求項14のスクランブル装置は、上記請求項10において、パケット廃棄に関する優先度が、MPEG2トランスポートストリームにおけるトランスポートパケットの優先度を示す1ビットのフラグtransport __priorityであることを特徴としている。効果制御を実現できるとともに、パケット廃棄に対する影響を低減できる。

【0040】本発明に係る請求項15のデスクランブル装置は、パケット廃棄に関する優先度に応じて異なるスクランブルモードでデスクランブルを行うように構成されていることを特徴としている。パケット廃棄に関する優先度によりスクランブルモードを変更することによって、効果制御を実現できるとともに、パケット廃棄に対する影響を低減することができる。

【0041】本発明に係る請求項16のデスクランブル装置は、上記請求項15において、優先度判定装置と暗

号解読装置とを具備し、前記優先度判定装置は、パケット廃棄に関する優先度を有するパケットを入力とし、入力されたパケットの前記パケット廃棄に関する優先度を判定し、前記暗号解読装置にパケットとスクランブルモード信号を出力するように構成され、前記暗号解読装置は、前記優先度判定装置からの前記スクランブルモード信号に基づきデスクランブルを行うように構成されていることを特徴としている。効果制御を実現できるとともに、パケット廃棄に対する影響を低減できる。

【0042】本発明に係る請求項17のデスクランブル装置は、上記請求項15において、スクランブル鍵を有する場合には、パケット廃棄に関する優先度が高優先度のパケットについてはデスクランブルを行わず、前記パケット廃棄に関する優先度が低優先度のパケットについてはデスクランブルを行い、かつ、前記スクランブル鍵を有しない場合には、前記パケット廃棄に関する優先度が高優先度のパケットについては処理を行わず、前記パケットに関する優先度が低優先度のパケットについては廃棄を行うように構成されていることを特徴としている。優先度の高いパケットに画像の低解像度の情報を、優先度の低いパケットに画像の低解像度の情報に追加する高解像度の情報をそれぞれ割り当てることによって、正規の受信者以外の受信者も低解像度の画像を視聴することが可能な効果制御を実現できる。

【0043】本発明に係る請求項18のデスクランブル装置は、上記請求項15において、連鎖のある暗号方式でデスクランブルを行い、パケット廃棄に関する優先度が高優先度のパケットと低優先度のパケットとを別々の前記連鎖のある暗号方式の系列としてデスクランブルを行うように構成されていることを特徴としている。パケット廃棄に関する優先度の高いパケットと低いパケットを別々の連鎖のある暗号方式の系列としてデスクランブルすることによって、ネットワーク中で優先度の低いパケットの廃棄が行われた場合にでも、優先度の高いパケットに影響を及ぼさないようにすることが可能となり、パケット廃棄への影響を低減することができる。

【0044】本発明に係る請求項19のデスクランブル装置は、上記請求項15において、パケット廃棄に関する優先度が、MPEG2トランスポートストリームにおけるトランスポートパケットの優先度を示す1ビットのフラグtransport __priorityであることを特徴としている。効果制御を実現できるとともに、パケット廃棄に対する影響を低減できる。

【0045】本発明に係る請求項20のスクランブル伝送装置用の信号処理装置は、パケット廃棄に関する優先度を有するパケットを入力とし、入力された2つの連続するパケットを単位として処理を行い、2つのパケットのうち一方のパケットのパケット廃棄に関する優先度が高優先度のパケットの場合には2つのパケットの両方を高優先度のパケットに書き換えてスクランブル装置に出

10

20

30

40

50

力するように構成されていることを特徴としている。2つずつの連続したパケットを単位として処理を行うスクランブル伝送装置において、優先度の低いパケットの廃棄が行われた場合も、同じパケット単位内には優先度の高いパケットは含まれないため、同じパケット単位内の優先度の高いパケットには影響がなく、優先度の高いパケット単位とは別の連鎖のある暗号方式の系列のため、次のパケット単位の優先度の高いパケットにも影響がない。

【0046】本発明に係る請求項21のスクランブル伝送装置用の信号処理装置は、パケット廃棄に関する優先度が、MPEG2トランスポートストリームにおけるトランスポートパケットの優先度を示す1ビットのフラグtransport __priorityであることを特徴としている。効果制御を実現できるとともに、パケット廃棄に対する影響を低減できる。

【0047】本発明に係る請求項22のスクランブル装置は、上記請求項8において、2つの連続するパケットを単位として処理を行うことに代えて、3つ以上の連続するパケットを単位として処理を行うように構成してあることを特徴としている。効果制御とパケット廃棄影響低減の効果に拡張性をもたせることができる。

【0048】本発明に係る請求項23のスクランブル伝送装置用の信号処理装置は、上記請求項20において、2つの連続するパケットを単位として処理を行うことに代えて、3つ以上の連続するパケットを単位として処理を行うように構成してあることを特徴としている。効果制御とパケット廃棄影響低減の効果に拡張性をもたせることができる。

【0049】以下、本発明の実施の形態に係るスクランブル伝送装置について図面に基づいて詳細に説明する。

【0050】〔実施の形態1〕図1は本発明の実施の形態1に係るスクランブル伝送装置の構成を示すブロック図である。

【0051】図1において、1aはデータの符号化を行う符号化装置、1bは原信号を入力とし、優先度の書き換えを行う信号処理装置、1cは信号処理装置1bからの信号とスクランブル鍵を入力とし、パケットの優先度に応じてスクランブルを行い出力するスクランブル装置、1dはパケットの優先度からスクランブルモードを決定し、スクランブルモード信号と原信号を出力する優先度判定装置、1eはスクランブル鍵と優先度判定装置1dからのスクランブルモード信号に基づき原信号をスクランブルする暗号化装置、1fはスクランブル信号をATMセルに変換し、ATMネットワーク上に出力するATMアダプター、1gはネットワークからのATMセルをもとのスクランブル信号に戻すATMアダプター、1hはスクランブル信号をデスクランブルし、原信号に戻すデスクランブル装置、1iはスクランブル信号の優先度とスクランブル鍵からスクランブルモードを決定し、スクランブルモード

信号とスクランブル信号を出力する優先度判定装置、1jはスクランブル鍵と優先度判定装置1iからのスクランブルモード信号に基づきスクランブル信号をデスクランブルする暗号解読装置、1kは符号化データの復号を行う復号化装置である。

【0052】以上のように構成された本実施の形態1のスクランブル伝送装置において、以下にその動作を説明する。

【0053】原信号はMPEG(Moving Picture Expert Group: 国際標準化機構ISOと国際電気標準会議IECの合同の作業グループ)標準の映像信号をMPEGシステムのトランスポートパケットにより多重化し、1ピクチャーに対応するトランスポートパケットをtransport __priority=1とし、PピクチャーおよびBピクチャーに対応するトランスポートパケットのtransport __priority=0とした信号であるとする。MPEG標準の詳細については、「最新MPEG教科書」(アスキー出版局編)にその解説がなされている。

【0054】以下に、MPEG標準に基づく映像信号のピクチャーの構成およびMPEGシステム層におけるトランスポートストリームについて説明する。

【0055】図2は、MPEG標準に準拠した映像信号のピクチャーの構造の説明図である。以下、MPEG標準におけるピクチャーの構造について説明する。図2において、5a, 5eがIピクチャー、5b, 5dがBピクチャー、5cがPピクチャーである。

【0056】図2のようにMPEG標準に準拠した映像信号は、3つのピクチャー、すなわち、Iピクチャー、Pピクチャー、Bピクチャーに分けられる。Iピクチャー5a, 5eは、その情報からだけで符号化された画面で、フレーム間予測を使わずに生成される。Pピクチャー5cは、IピクチャーまたはPピクチャーからの順方向予測を行うことによってできる画面で、単独では復号することはできない。Bピクチャー5b, 5dは、過去のIピクチャーまたはPピクチャーからの順方向予測と未来のIピクチャーまたはPピクチャーからの逆方向予測とを合わせた双方向予測を行うことによってできる画面で、単独では復号することはできない。

【0057】以下、MPEG標準のシステムストリームにおけるトランスポートストリームについて説明する。図3は、MPEG標準に準拠したトランスポートパケットの構成図である。図3において、6aはトランスポートパケットである。トランスポートストリームは、長さ188byteのトランスポートパケット6aからなり、トランスポートパケット6aは、基本的に4byteのヘッダと、184byteのペイロードからなる。

【0058】次に、トランスポートパケットヘッダ中のシンタックスについて説明する。まず、PIDは、ペイロードに含まれる情報の区別を行い、このシンタックスにより、映像信号か音声信号かなどの判別が可能とな

る。また、transport __priorityは、そのトランスポートの優先度を示す1bitのフラグであり、次に述べるATM伝送への対応などの目的に用いられる。また、transport __scrambling_controlによりパケットにスクランブルかかかっているかどうかなどのパケットのスクランブル情報が示される。

【0059】ネットワーク上の伝送方式としては、ATM (Asynchronous Transfer Mode: 非同期転送モード) 伝送を用い、ATMセル上にMPEG信号を割り当てる方式としてMPEG over ATMを用いるものとする。ATM伝送およびMPEG over ATMの詳細については、「標準ATM教科書」(アスキー出版局編)にその解説がなされている。

【0060】以下に、ATM伝送について説明する。

【0061】図4はATM伝送で用いられるATMセルの構成図である。図4において、7aはATMセルである。ATM伝送では、情報をATMセルと呼ばれる固定長のセルに分解して伝送することにより高速伝送を実現する。ATMセルは、図4に示すとおり53byteの固定長であり、5byteのヘッダと48byteのペイロードをもつ。ATM伝送においては、原理上、セル廃棄すなわちネットワーク上で輻輳などのためセルを廃棄する必要があることがあるが、この際、ヘッダ中のCell Loss Priorityが用いられる。Cell Loss Priorityは、1bitのシンタックスで、セルが高優先であるか低優先であることを示す。ATMネットワークでは、セル廃棄の必要が生じた場合には、このCell Loss Priorityを見て、優先度の低いセルを先に廃棄するようにする。

【0062】次に、MPEG over ATMについて説明する。MPEG over ATMとは、先に説明したMPEG標準におけるトランスポートストリームのトランスポートパケットをATM伝送で伝送する際の方式である。MPEG over ATMの方式としては現在、AAL1、AAL5の2つの方式が考えられている。以下、AAL1、AAL5の2つのMPEG over ATMの方式について説明する。

【0063】図5はAAL1によるMPEG over ATMの方式の説明図である。図5において、8aはトランスポートパケット、8b、8c、8d、8eはATMセルである。図5に示すように、AAL1では、188byteのトランスポートパケット8aを47byteのブロック4つに分割し、ATMセル8b、8c、8d、8eのペイロードに配置する。

【0064】また、AAL5によるMPEG over ATMの方式では、図6で示したように、MPEGのトランスポートパケット4a、4bの2つを単位として、これにCRCを含むCPCS-PDUトレーラー4cを加えたものを8つのATMセル4d、4e、4f、4g、4h、4i、4j、4kのペイロードに割り当てる。

【0065】また、暗号方式としては、暗号文ブロック

連鎖方式(CBCモード)を用いる。

【0066】以上のような原信号、伝送方式、暗号方式を扱う本実施の形態1について、図1に戻って以下にその動作を説明する。

【0067】送信側では、データの符号化、スクランブル、送信を行う。

【0068】まず、符号化装置1aにおいて、MPEG標準の映像信号を生成し、Iピクチャーに対応するデータをパケット廃棄に関する優先度の高いトランスポートパケットとして、すなわちtransport __priority=1のトランスポートパケットとして、また、PピクチャーおよびBピクチャーに対応するデータをパケット廃棄に関する優先度の低いトランスポートパケットとして、すなわちtransport __priority=0のトランスポートパケットとして、信号処理装置1bに出力する。

【0069】実施の形態1においては、信号処理装置1bでは、処理を行わず、符号化装置1aからの原信号をそのまま出力する。

【0070】信号処理装置1bからの信号を受けとったスクランブル装置1cでは、優先度の低いパケットに対してスクランブルを行う。信号は、まず、優先度判定装置1dに入力され、ここで、トランスポートパケット中のtransport __priorityを見て、0の場合にはスクランブルを行うスクランブルモード信号を、1の場合にはスクランブルを行わないスクランブルモード信号を暗号化装置1eに出力する。暗号化装置1eでは、スクランブルモード信号とスクランブル鍵に基づきトランスポートパケット単位に処理を行う。スクランブルモード信号がスクランブルを示す信号の場合には、スクランブル鍵に基づきトランスポートパケットのスクランブルを行い、スクランブルモード信号がノンスクリンブルを示す信号の場合にはトランスポートパケットをそのまま出力する。

【0071】ATMアダプター1fでは、スクランブル装置1cからのトランスポートパケットをATMセルに変換し出力する。図5に示すMPEG over ATMのAAL1を用いて、トランスポートパケットを4つのATMセルに分割して送信を行う。この際、ATMアダプター1fでは、transport __priority=1のトランスポートパケットはCell Loss Priority=1のATMセルとして、transport __priority=0のトランスポートパケットはCell Loss Priority=0のATMセルとして出力する。

【0072】次に、受信側の動作について説明する。受信側では、受信、デスクランブル、データの復号化を行う。

【0073】ATMアダプター1gでは、ネットワークからのATMセルをトランスポートパケットに変換する。図5に示すMPEG over ATMのAAL1を用い、分割した4つのATMセルを1つのトランスポートパケットに戻し、トランスポートパケットを出力する。

この際、ATMアダプター1gでは、Cell Loss Priority = 1 の ATMセルはtransport __priority=1 のトランスポートパケットとして、Cell Loss Priority=0 の ATMセルはtransport __priority=0 のトランスポートパケットとして出力する。

【0074】次に、デスクランブル装置1hでは、契約を行っていて視聴可能な場合には、優先度の低いパケットについてはデスクランブルを行い、優先度の高いパケットは処理を行わずそのまま出力する。契約を行っておらず視聴不可の場合には、優先度の低いパケットは削除して、優先度の高いパケットのみ処理せずにそのまま出力する。スクランブルされたトランスポートパケットを入力した優先度判定装置1iでは、契約を行っていて視聴可能な場合（スクランブル鍵が存在する場合）には、transport __priorityを見て、transport __priority=1 の場合はスクランブルモード信号を処理しないモードに、transport __priority=0 の場合はスクランブルモード信号をデスクランブルするモードにし、契約を行っておらず視聴不可能な場合（スクランブル鍵が存在しない場合）には、transport __priority=1 の場合はスクランブルモード信号を処理しないモードに、transport __priority=0 の場合はスクランブルモード信号をパケット廃棄を行うモードにして出力する。暗号解読装置1jでは、スクランブルモード信号を見て、スクランブルモード信号が処理しないモードの場合にはトランスポートパケットの処理は行わず、スクランブルモード信号がデスクランブルモードの場合にはスクランブル鍵をもとにデスクランブルを行い、スクランブルモード信号がパケット廃棄の場合にはトランスポートパケットをNULLパケットに置き換えて出力する。

【0075】復号化装置1kは、デスクランブル装置1hの出力を受け取り、データの復号を行う。

【0076】以上のような動作により、本実施の形態1では、正規の受信者は、Iピクチャー、PピクチャーおよびBピクチャーのすべてのピクチャーを復号することが可能となり、正常の動画像を得ることができる。また、正規の受信者以外の受信者は、優先度の高いトランスポートパケットのみを得て、Iピクチャーのみを復号することが可能となり、正規の受信者以外もある程度の画像を得ることのできる効果制御を実現できる。

【0077】また、本実施の形態1においては、優先度を示す1ビットのフラグtransport __priorityをスクランブルのON/OFFの制御に用いることができるため、2bit のシンタックスtransport __scrambling_control をON/OFF以外の制御に2bit 使うことができるという利点もある。

【0078】なお、スクランブル鍵は公知の手段で伝送を行うことができる。

【0079】また、本実施の形態1では、符号化装置1aでの優先度の割り当ての方法として、Iピクチャーを優

先度の高いパケットに、PピクチャーおよびBピクチャーを優先度の低いパケットに割り当てる方法を1例として挙げたが、優先度の高いパケットに対応する情報が単独で復号可能な他のいかなる割り当て法でも効果制御を実現することができる。他の例としては、階層符号化方式であるMPEGのスケラビリティを用いて、高位レイヤの画像を優先度の低いトランスポートパケットに、低位レイヤの画像を優先度の高いトランスポートパケットに割り当て、正規の受信者以外が低位レイヤの画像のみを視聴することができるようにする方法や、DCT（離散コサイン変換）成分の交流成分の情報を優先度の低いトランスポートパケットに、それ以外の情報を優先度の高いトランスポートパケットに割り当てることにより、正規の受信者以外が直流成分のみを含むモザイク状の画像を視聴することができるようにする方法などがある。また、本方式がMPEG以外のパケット廃棄に関する優先度を含む信号を出力する映像、音声などのデータ信号すべてに対して有効であることはいうまでもない。

【0080】なお、本実施の形態1では、ネットワークの伝送方法として、ATM（非同期転送モード）による伝送の例を挙げたが、他のいかなる伝送方法においてもまた記録メディアにおいても、本発明は有効である。

【0081】また、本実施の形態1では、暗号方式として、暗号化ブロック連鎖方式（CBCモード）を例として挙げたが、他のいかなる暗号方式においても、本発明は有効である。

【0082】〔実施の形態2〕次に、本発明の実施の形態2に係るスクランブル伝送装置について説明する。

【0083】実施の形態2の説明においては、実施の形態1の説明で用いた図1を利用する。

【0084】原信号はMPEG標準の映像信号をMPEGシステムのトランスポートパケットにより多重化し、Iピクチャーに対応するトランスポートパケットをtransport __priority=1、PピクチャーおよびBピクチャーに対応するトランスポートパケットをtransport __priority=0とした信号であるとする。次に、ネットワーク上の伝送方式としてはATM伝送を用い、ATMセル上にMPEG信号を割り当てる方式としてMPEG over ATMのAAL1（図5参照）を用いるものとする。また、暗号方式としては暗号文ブロック連鎖方式（CBC）を用いる。

【0085】以上のような原信号、伝送方式、暗号方式を扱う本実施の形態2について、図1を用いて以下にその動作を説明する。

【0086】送信側では、データの符号化、スクランブル、送信を行う。

【0087】まず、符号化装置1aにおいて、MPEG標準の映像信号を生成し、Iピクチャーに対応するデータをパケット廃棄に関する優先度の高いトランスポートパ

10

20

30

40

50

ケットとして、すなわちtransport __priority=1のトランスポートパケットとして、PピクチャーおよびBピクチャーに対応するデータをパケット廃棄に関する優先度の低いトランスポートパケットとして、すなわちtransport __priority=0のトランスポートパケットとして信号処理装置1bに出力する。

【0088】実施の形態2においては、信号処理装置1bでは処理を行わず、符号化装置1aからの原信号をそのまま出力する。

【0089】信号処理装置1bからの信号を受け取ったスクランブル装置1cでは、優先度の高いパケットと優先度の低いパケットとを別々の連鎖のある暗号方式の系列としてスクランブルを行う。この動作を図7を用いて説明する。図7において、9a、9c、9eは優先度の高いパケット、9b、9dは優先度の低いパケットである。暗号化装置1eは、優先度の高いパケットと優先度の低いパケットのそれぞれに対するCBCレジスタを用意するものし、図7に示すように、優先度の高いパケットのスクランブルを行うときには、前の優先度の高いパケットのCBCレジスタの値を用いてスクランブルを行い（CBC系列2）、優先度の低いパケットのスクランブルを行うときには、前の優先度の低いパケットのCBCレジスタの値を用いてスクランブルを行う（CBC系列1）ことによって、優先度の高いパケットと優先度の低いパケットを別々の系列の連鎖のある暗号方式としてスクランブルを行う。スクランブル装置1cに入力された原信号は、優先度判定装置1dに入力され、ここで、トランスポートパケット中のtransport __priorityを見て、1の場合には優先度の高いパケットを示すスクランブルモード信号を、0の場合には優先度の低いパケットを示すスクランブルモード信号を暗号化装置1eに出力する。暗号化装置1eでは、スクランブルモード信号とスクランブル鍵に基づきトランスポートパケット単位に処理を行う。スクランブルモード信号が優先度の高いパケットを示す信号の場合には、優先度の高いパケット用のCBCレジスタを用いて、スクランブル鍵に基づき暗号文ブロック連鎖方式（CBCモード）でトランスポートパケットのスクランブルを行い、スクランブルモードが優先度の低いパケットの場合には、優先度の低いパケット用のCBCレジスタを用いて、スクランブル鍵に基づき暗号文ブロック暗号方式でトランスポートパケットのスクランブルを行う。また、この際、スクランブル装置1cは、transport __scrambling_controlをONにして出力を行う。

【0090】ATMアダプター1fでは、スクランブル装置1cからのトランスポートパケットをATMセルに変換し、出力する。図5に示すMPEG over ATMのAAL1を用いてトランスポートパケットを4つのATMセルに分割し、送信を行う。この際、ATMアダプター1fでは、transport __priority=1のトランスポートパケットはCell Loss Priority=1のATMセルとし

て、transport __priority=0のトランスポートパケットはCell Loss Priority=0のATMセルとして出力する。

【0091】次に、受信側の動作について説明する。受信側では、受信、デスクランブル、データの復号化を行う。

【0092】ATMアダプター1gでは、ネットワークからのATMセルをトランスポートパケットに変換する。図5に示すMPEG over ATMのAAL1を用い、分割した4つのATMセルを1つのトランスポートパケットに戻し、トランスポートパケットを出力する。この際、ATMアダプター1gでは、Cell Loss Priority=1のATMセルはtransport __priority=1のトランスポートパケットとして、Cell Loss Priority=0のATMセルはtransport __priority=0のトランスポートパケットとして出力する。

【0093】この信号を受け取ったデスクランブル装置1hでは、図7に示したように優先度の高いパケットと優先度の低いパケットとを別々の連鎖のある暗号方式の系列としてデスクランブルを行う。デスクランブル装置1hに入力された信号は、優先度判定装置1iに入力され、ここで、トランスポートパケット中のtransport __priorityを見て、1の場合には優先度の高いパケットを示すスクランブルモード信号を、0の場合には優先度の低いパケットを示すスクランブルモード信号を暗号解読装置1jに出力する。暗号解読装置1jでは、スクランブルモード信号とスクランブル鍵に基づきトランスポートパケット単位に処理を行う。スクランブルモード信号が優先度の高いパケットを示す信号の場合には、優先度の高いパケット用のCBCレジスタを用いて、スクランブル鍵に基づき暗号文ブロック連鎖方式（CBCモード）でトランスポートパケットのデスクランブルを行い、スクランブルモード信号が優先度の低いパケットの場合には、優先度の低いパケット用のCBCレジスタを用いて、スクランブル鍵に基づき暗号文ブロック連鎖方式（CBCモード）でトランスポートパケットのデスクランブルを行う。また、この際、デスクランブル装置1hは、transport __scrambling_controlをOFFにして出力を行う。

【0094】復号化装置1kは、デスクランブル装置1hの出力を受け取り、データの復号を行う。

【0095】以上のような動作により、この実施の形態2では、パケットの廃棄に対する影響を低減したスクランブル伝送装置を実現することができる。すなわち、ATMネットワーク上でセル廃棄が行われた場合に、優先度の異なるトランスポートパケットを同じ連鎖のある暗号方式の系列としてスクランブルを行った場合には、図10で示したように、次の優先度の高いパケットがデスクランブルできない可能性がある。しかしながら、本実施の形態2のようなスクランブル伝送装置によれば、優先度の低いパケットが廃棄された場合にも、優先度の高

いパケットがデスクランブルできない可能性はなくなり、パケット廃棄の影響を低減したスクランブル伝送装置を実現できる。本実施の形態2のように、Iピクチャーに対応するデータをパケット廃棄に関する優先度の高いトランスポートパケットとし、PピクチャーおよびBピクチャーに対応するデータをパケット廃棄に関する優先度の低いトランスポートパケットとした場合には、相対的に重要な情報であるIピクチャーのデータは失われないため、ATMネットワークにおいてパケット廃棄が行われた場合にも、乱れの少ない画像を受信者は視聴することができる。

【0096】なお、スクランブル鍵は公知の手段で伝送を行うことができる。

【0097】また、本実施の形態2では、符号化装置1aでの優先度の割り当ての方法として、Iピクチャーを優先度の高いパケットに、PピクチャーおよびBピクチャーを優先度の低いパケットに割り当てる方法を1例として挙げたが、他のいかなる割り当て法においても本発明は有効である。更に、本方式がMPEG以外のパケット廃棄に関する優先度をもつ信号を出力する映像、音声などのデータ信号すべてに有効であることはいうまでもない。

【0098】なお、本実施の形態2では、ネットワークの伝送方法としてATM（非同期転送モード）による伝送の例を挙げたが、他のいかなるパケット廃棄が行われる伝送方法においてもまた記録メディアにおいても、本発明は有効である。

【0099】また、本実施の形態2では、暗号方式として、暗号文ブロック連鎖方式（CBCモード）を例として挙げたが、他のいかなる連鎖のある暗号方式においても、本発明は有効である。

【0100】〔実施の形態3〕次に、本発明の実施の形態3に係るスクランブル伝送装置について説明する。実施の形態3の説明においては、実施の形態1の説明で用いた図1を利用する。

【0101】原信号はMPEG標準の映像信号をMPEGシステムのトランスポートパケットにより多重化し、Iピクチャーに対応するトランスポートパケットをtransport __priority=1とし、PピクチャーおよびBピクチャーに対応するトランスポートパケットをtransport __priority=0とした信号であるとする。次に、ネットワーク上の伝送方式としては、ATM伝送を用い、ATMセル上にMPEG信号を割り当てる方式としてMPEG over ATMのAAL5を用いるものとする。また、暗号方式としては、暗号文ブロック連鎖方式（CBCモード）を用いる。

【0102】以上のような原信号、伝送方式、暗号方式を扱う本実施の形態3について、図1を用いて以下にその動作を説明する。

【0103】送信側では、データの符号化、スクランブル

ル、送信を行う。

【0104】まず、符号化装置1aにおいて、MPEG準拠の映像信号を生成し、Iピクチャーに対応するデータをパケット廃棄に関する優先度の高いトランスポートパケットとして、すなわちtransport __priority=1のトランスポートパケットとして、また、PピクチャーおよびBピクチャーに対応するデータをパケット廃棄に関する優先度の低いトランスポートパケットとして、すなわちtransport __priority=0のトランスポートパケットとして信号処理装置1bに出力する。

【0105】次に、この信号処理装置1bからの信号を、送信側でどのように処理するかを以下に図8を用いて説明する。図8において、10a, 10e, 10f, 10i, 10m, 10n, 10q, 10r, 10u, 10v は優先度の高い優先パケット、10b, 10c, 10d, 10g, 10h, 10j, 10k, 10l, 10o, 10p, 10s, 10t, 10w, 10x は優先度の低い非優先パケットである。図8に示すように、パケットは2つを単位として処理が行われ、信号処理装置1bにおいて、優先度の高いパケットを1つ含むパケット単位は、両方のパケットが優先度の高いパケットに書き換えられる。

【0106】次にスクランブル装置1cにおいては、優先度の高いパケット単位は、優先度の高いパケットを含む前のパケット単位の系列（CBC系列2）のCBCレジスタの値を用いてスクランブルが行われ、優先度の高いパケットを含まないパケット単位は、前の優先度の高いパケットを含まないパケット単位の系列（CBC系列1）のCBCレジスタの値を用いてスクランブルが行われる。以上のような動作により、送信側では、優先度の高いパケットを含むパケット単位と優先度の高いパケットを含まないパケット単位を、別々の系列の暗号文ブロック連鎖方式（CBCモード）としてスクランブルを行う。

【0107】符号化装置1aからの原信号を受け取った信号処理装置1bでは、2つのトランスポートパケット単位に処理を行い、トランスポートパケット2つのうち一方が優先度の高いパケットの場合には、2つとも優先度の高いパケットに書き換える。

【0108】この様子が図8に示されている。例えば、優先パケット10a と非優先パケット10b とからなるパケット単位ではそれぞれが優先パケット10m と優先パケット10nになる。また、優先パケット10e と優先パケット10f とからなるパケット単位ではそれぞれがもとと同じ優先パケット10q と優先パケット10r になる。また、非優先パケット10c と非優先パケット10d とからなるパケット単位ではそれぞれがもとと同じ非優先パケット10o と非優先パケット10p になる。

【0109】信号処理装置1bからの信号を受け取ったスクランブル装置1cでは、優先度の高いパケットと優先度の低いパケットとを別々の暗号文ブロック連鎖方式（C

BCモード)の系列としてスクランブルを行う。スクランブル装置1cに入力された信号は優先度判定装置1dに入力され、トランスポート packets 中のtransport __priorityを見て、1の場合には優先度の高い packets を示すスクランブルモード信号を、0の場合には優先度の低い packets を示すスクランブルモード信号を暗号化装置1eに出力する。暗号化装置1eでは、スクランブルモード信号とスクランブル鍵に基づきトランスポート packets 単位に処理を行う。スクランブルモード信号が優先度の高い packets を示す信号の場合には、優先度の高い packets 用のCBCレジスタを用いて、スクランブル鍵に基づき暗号文ブロック連鎖方式(CBCモード)でトランスポート packets のスクランブルを行い、スクランブルモードが優先度の低い packets の場合には、優先度の低い packets 用のCBCレジスタを用いて、スクランブル鍵に基づき暗号文ブロック連鎖方式でトランスポート packets のスクランブルを行う。また、この際、スクランブル装置1cは、transport __scrambling_control をONにして出力を行う。

【0110】ATMアダプター1fは、スクランブル装置1cからのスクランブルされたトランスポート packets をATMセルに変換し、出力する。図6に示すMPEG over ATMのAAL5を用いて、単位となっているトランスポート packets 2つとCRCなどを含むCPCS-PDUトレーラーを、ATMセル8つに分割して送信を行う。この際、ATMアダプター1fでは、transport __priority=1のトランスポート packets はCell Loss Priority=1のATMセルとして、transport __priority=0のトランスポート packets はCell Loss Priority=0のATMセルとして出力する。

【0111】次に、受信側の動作について説明する。受信側では、受信、デスクランブル、データの復号化を行う。

【0112】ATMアダプター1gでは、ネットワークからのATMセルをトランスポート packets に変換する。図6に示すMPEG over ATMのAAL5を用い、分割した8つのATMセルを2つのトランスポート packets に戻し、トランスポート packets を出力する。この際、ATMアダプター1gでは、Cell Loss Priority=1のATMセルはtransport __priority=1のトランスポート packets として、Cell Loss Priority=0のATMセルはtransport __priority=0のトランスポート packets として出力する。

【0113】この信号を受け取ったデスクランブル装置1hでは、図8に示したように優先度の高い packets と優先度の低い packets とを別々の連鎖のある暗号方式の系列としてデスクランブルを行う。デスクランブル装置1hに入力されたスクランブル信号は優先度判定装置1iに入力され、ここでトランスポート packets 中のtransport __priorityを見て、1の場合には優先度の高い packets

を示すスクランブルモード信号を、0の場合には優先度の低い packets を示すスクランブルモード信号を暗号解読装置1jに出力する。暗号解読装置1jでは、スクランブルモード信号とスクランブル鍵に基づきトランスポート packets 単位に処理を行う。スクランブルモード信号が優先度の高い packets を示す信号の場合には、優先度の高い packets 用のCBCレジスタを用いて、スクランブル鍵に基づき暗号文ブロック連鎖方式(CBCモード)でトランスポート packets のデスクランブルを行い、スクランブルモードが優先度の低い packets の場合には、優先度の低い packets 用のCBCレジスタを用いて、スクランブル鍵に基づき暗号文ブロック連鎖方式でトランスポート packets のデスクランブルを行う。また、この際、デスクランブル装置1hは、transport __scrambling_control をOFFにして出力を行う。

【0114】復号化装置1kは、デスクランブル装置1hの出力を受け取り、データの復号を行う。

【0115】以上のような動作により、この実施の形態3では、MPEG over ATMのAAL5などのように複数 packets を単位としてネットワークにおける伝送を行う場合に、 packets の廃棄に対する影響を低減したスクランブル伝送装置を実現することができる。すなわち、これまでは、ATMネットワーク上で優先度の低いセルの廃棄が行われた場合、そのATMセルを含むトランスポート packets は復号不可能となり、従って、AAL5でそのトランスポート packets とペアになっていたトランスポート packets も復号不可能となる。更に暗号文ブロック連鎖方式(CBCモード)を用いている場合には、同じ連鎖上の次のトランスポート packets も復号不可能となる。しかし、本実施の形態3におけるスクランブル伝送装置では、優先度の低いセルが廃棄され、そのセルを含むトランスポート packets が復号不可能となった場合にも、AAL5上でペアとなっているトランスポート packets は優先度の低いトランスポート packets であり、連鎖上で次のトランスポート packets も優先度の低い packets であるため、影響が少ないという効果がある。

【0116】本実施の形態3のように、Iピクチャーに対応するデータを packets 廃棄に関する優先度の高いトランスポート packets とし、PピクチャーおよびBピクチャーに対応するデータを packets 廃棄に関する優先度の低いトランスポート packets とした場合には、相対的に重要な情報であるIピクチャーのデータは失われないため、 packets 廃棄が行われた場合にも、乱れの少ない画像を受信者は視聴することができる。

【0117】なお、スクランブル鍵は公知の手段で伝送を行うことができる。

【0118】また、本実施の形態3では、符号化装置1aでの優先度の割り当ての方法として、Iピクチャーを優先度の高い packets に、PピクチャーおよびBピクチャー

一を優先度の低いパケットに割り当てる方法を1例として挙げたが、他のいかなる割り当て法に対しても本発明は有効である。更に、本方式がMPEG以外のパケット廃棄に関する優先度をもつ信号を出力する映像、音声などのデータ信号すべてに有効であることはいうまでもない。

【0119】なお、本実施の形態3では、ネットワークの伝送方法としてATM（非同期転送モード）による伝送の例を挙げたが、他のいかなるパケット廃棄が行われる伝送方法においてもまた記録メディアにおいても、本発明は有効である。

【0120】また、本実施の形態3では、暗号方式として、暗号文ブロック連鎖方式（CBCモード）を例として挙げたが、他のいかなる連鎖のある暗号方式においても、本発明は有効である。

【0121】なお、本実施の形態3では、符号化装置1aの出力するパケットを2つ単位で処理してネットワーク中の伝送するMPEG over ATMのAAL5を例として挙げたが、2つ以上の単位でパケットを処理するいかなる処理に対しても、本発明は有効である。

【0122】更に、本発明の他の実施の形態としては、符号化装置の処理速度に比べて、スクランブル装置、デスクランブル装置の処理速度が遅く、すべてのパケットの処理を行うことができない場合に、優先度を用いて、高優先のパケットのみをスクランブルする実施の形態などが考えられ、本発明の実用的意義は大きい。

【0123】

【発明の効果】本発明に係るスクランブル伝送装置によれば、パケット廃棄に関する優先度をもつパケットにより構成される信号を入力とし、優先度に応じてスクランブルモードの切り換えを行ってスクランブルを行うスクランブル装置と、スクランブル装置からのスクランブル信号を入力とし、優先度に応じてスクランブルモードの切り換えを行ってデスクランブルを行うデスクランブル装置とから構成されており、パケット廃棄に関する優先度によりスクランブルモードを変更することによって、効果制御を実現できるとともに、パケット廃棄に対する影響を低減することができる。

【0124】また、パケット廃棄に関する優先度をもつパケットにより構成される信号を入力とし、優先度の高いパケットについてはスクランブルを行わず、優先度の低いパケットについてはスクランブルを行うスクランブル装置と、スクランブル装置からのスクランブル信号を入力とし、スクランブル鍵が存在する場合には優先度の低いパケットについてのみデスクランブルを行い、スクランブル鍵が存在しない場合には優先度の低いパケットを廃棄するデスクランブル装置とから構成されており、スクランブル装置においてパケット廃棄に関する優先度が低いパケットのみをスクランブルし、デスクランブル装置において、スクランブル鍵が存在する場合、すなわ

ち視聴などの契約を行っている場合にはデスクランブルを行い、スクランブル鍵が存在しない場合、すなわち視聴などの契約を行っていない場合にはデスクランブル不可能な優先度の低いパケットは廃棄する。このようにすることによって、正規の受信者は優先度の高いパケットと優先度の低いパケットの両方を復号することができ、正規の受信者以外の受信者は優先度の高いパケットのみを復号することができる。従って、例えば原信号がデジタル映像信号のような信号の場合に、優先度の高いパケットに画像の低解像度の情報を、優先度の低いパケットに画像の低解像度の情報に追加する高解像度の情報をそれぞれ割り当てることによって、正規の受信者以外の受信者も低解像度の画像を視聴することが可能な効果制御を実現することができる。

【0125】また、パケット廃棄に関する優先度をもつパケットにより構成される信号を入力とし、優先度の高いパケットと優先度の低いパケットを別々の連鎖のある暗号方式の系列としてスクランブルを行うスクランブル装置と、スクランブル装置からのスクランブル信号を入力とし、優先度の高いパケットと優先度の低いパケットを別々の連鎖のある暗号方式の系列としてデスクランブルを行うデスクランブル装置とから構成されており、パケット廃棄に関する優先度の高いパケットと低いパケットを別々の連鎖のある暗号方式の系列としてスクランブルすることによって、ネットワーク中で優先度の低いパケットの廃棄が行われた場合にも、優先度の高いパケットに影響を及ぼさないようにすることが可能となり、パケット廃棄への影響を低減することができる。

【0126】また、パケット廃棄に関する優先度をもつパケットにより構成される信号を入力とし、2つの連続するパケットを単位として処理し、2つのパケットのうち一方が優先度の高いパケットの場合には、両方とも優先度の高いパケットに書き換えて出力する信号処理装置と、信号処理装置からの信号を入力とし、優先度の高いパケットと優先度の低いパケットを別々の連鎖のある暗号方式の系列としてスクランブルを行うスクランブル装置と、スクランブル装置からのスクランブル信号を入力とし、優先度の高いパケットと優先度の低いパケットを別々の連鎖のある暗号方式の系列としてデスクランブルを行うデスクランブル装置とから構成されており、2つずつの連続したパケットを単位として処理を行うスクランブル伝送装置において、2つのパケットのうち一方が優先度の高いパケットの場合に両方とも優先度の高いパケットに書き換え、優先度の高いパケット単位と優先度の低いパケット単位とを別々の連鎖のある暗号方式の系列としてスクランブルし、優先度の低いパケットの廃棄の影響を低減することができる。すなわち、優先度の低いパケットの廃棄が行われた場合も、同じパケット単位内には優先度の高いパケットは含まれないため、同じパケット単位内の優先度の高いパケットには影響がなく、

優先度の高いパケット単位とは別の連鎖のある暗号方式の系列のため、次のパケット単位の優先度の高いパケットにも影響がない。

【図面の簡単な説明】

【図1】本発明の実施の形態1におけるスクランブル伝送装置の構成図である。

【図2】MPEG標準に準拠した映像信号のピクチャーの構成図である。

【図3】MPEG標準に準拠したトランスポートパケットの構成図である。

【図4】ATMセルの構成図である。

【図5】AAL1によるMPEG over ATMの方式の説明図である。

【図6】AAL5によるMPEG over ATMの方式の説明図である。

【図7】本発明の実施の形態2におけるスクランブル伝送装置の動作説明図である。

【図8】本発明の実施の形態3におけるスクランブル伝送装置の動作説明図である。

【図9】従来の技術における連鎖のあるブロック暗号方式（CBCモード）の説明図である。

【図10】従来の技術におけるパケット廃棄による影響の問題の説明図である。

【符号の説明】

1a……符号化装置

1b……信号処理装置

*

* 1c……スクランブル装置

1d……優先度判定装置

1e……暗号化装置

1f……ATMアダプター

1g……ATMアダプター

1h……デスクランブル装置

1i……優先度判定装置

1j……暗号解読装置

1k……復号化装置

10 4a, 4b……トランスポートパケット

4c……CPCS-PDUトレーラー

4d, 4e, 4f, 4g, 4h, 4i, 4j, 4k……ATMセル

5a, 5e……Iピクチャー

5b, 5d……Bピクチャー

5c……Pピクチャー

6a……トランスポートパケット

7a……ATMセル

8a……トランスポートパケット

8b, 8c, 8d, 8e……ATMセル

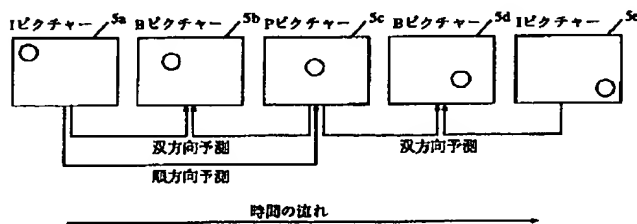
20 9a, 9c, 9e……優先パケット

9b, 9d……非優先パケット

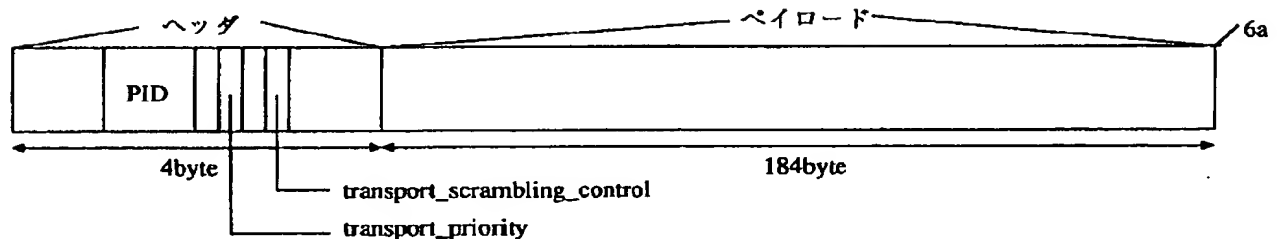
10a, 10e, 10f, 10i, 10m, 10n, 10q, 10r, 10u, 10v……優先パケット

10b, 10c, 10d, 10g, 10h, 10j, 10k, 10l, 10o, 10p, 10s, 10t, 10w, 10x……非優先パケット

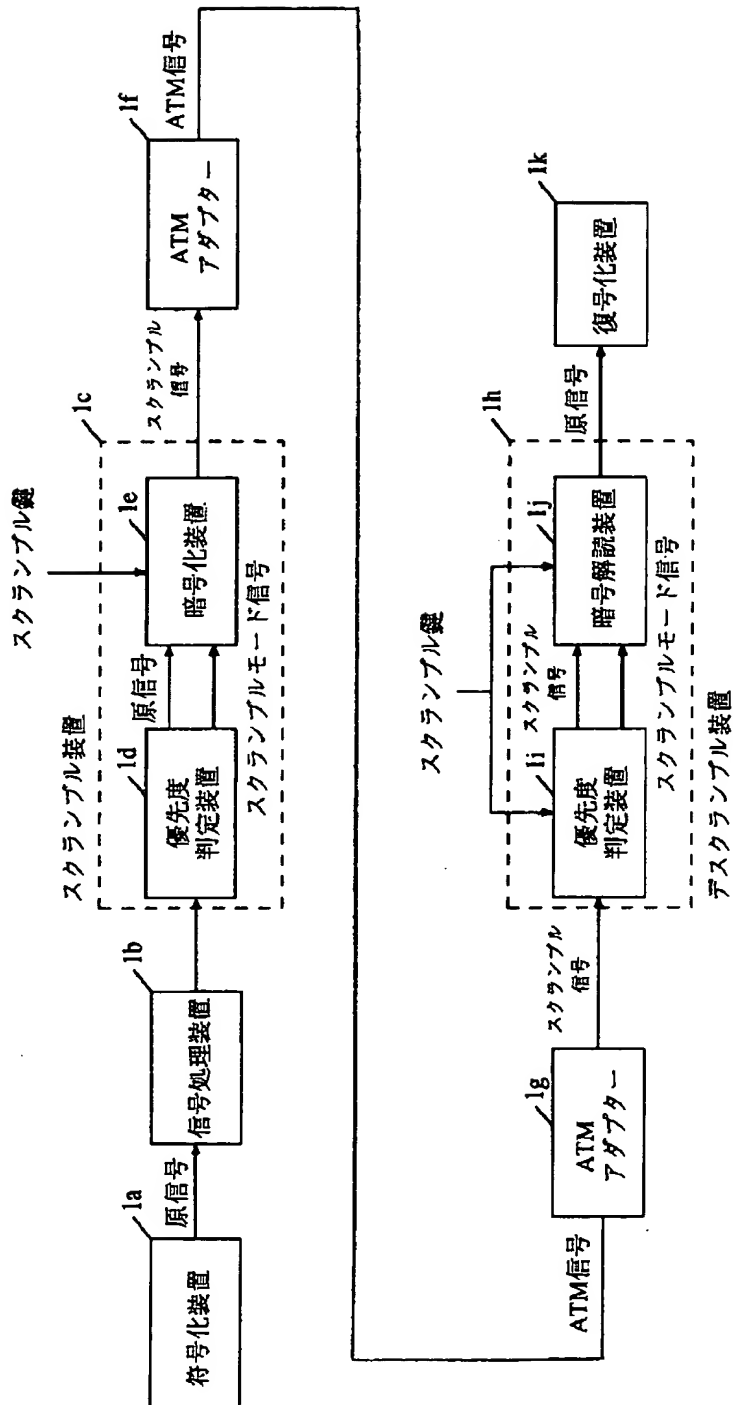
【図2】



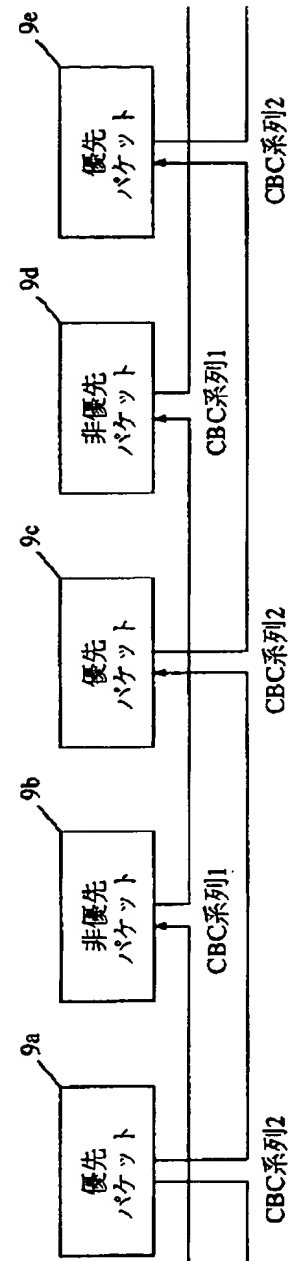
【図3】



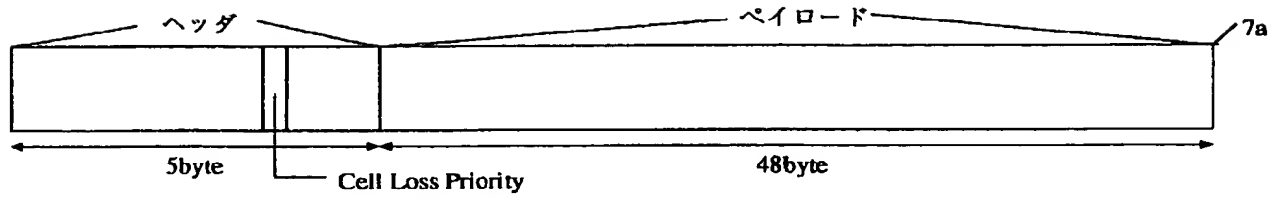
【図 1】



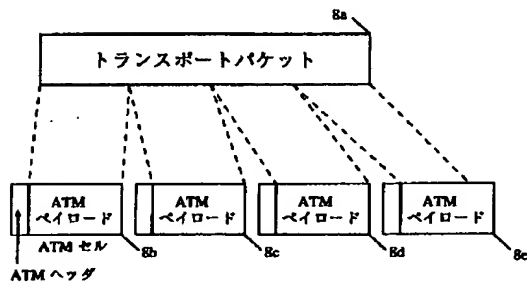
【図 7】



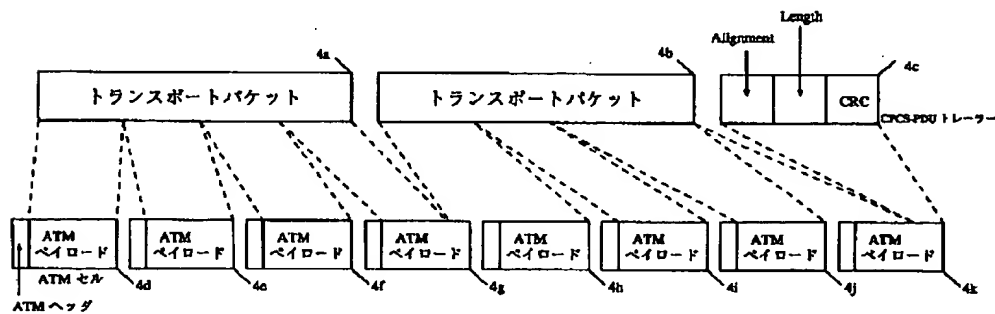
【図 4】



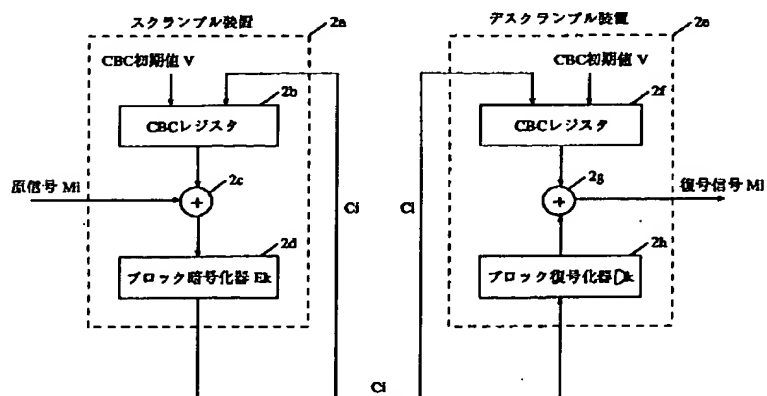
【図 5】



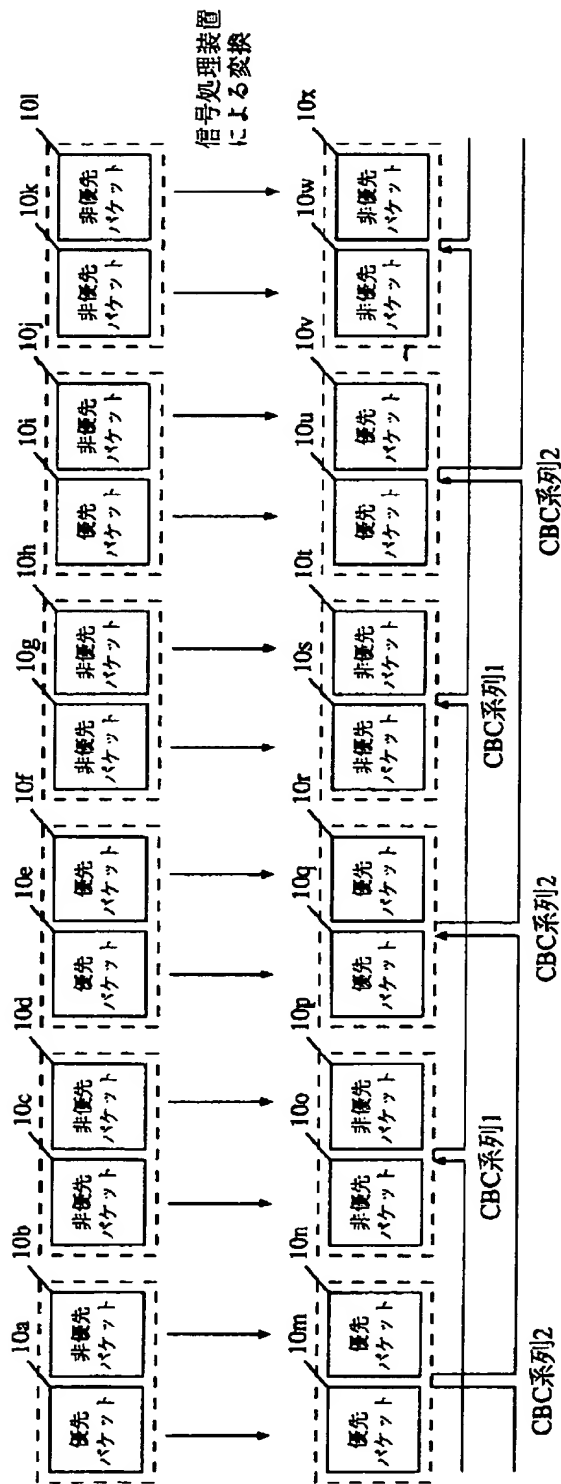
【図 6】



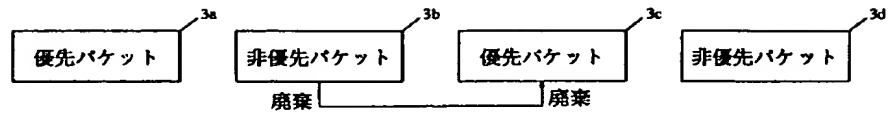
【図 9】



【図 8】



【図 1 0】



フロントページの続き

(72)発明者 茨木 晋
大阪府門真市大字門真1006番地 松下電器
産業株式会社内